PATENT ABSTRACTS OF JAPAN

(11)Publication number : 04-267462

(43)Date of publication of application : 24.09.1992

---

(51)Int.Cl. G06F 15/00
G06F 1/00
H04L 9/00
H04L 9/10
H04L 9/12

---

(21)Application number : 03-028226 (71)Applicant : CANON INC

(22)Date of filing : 22.02.1991 (72)Inventor : FUKUTOME NAOFUMI

---

(54) SECURITY SYSTEM

(57)Abstract:

PURPOSE: To capable of protecting security even when information such as user ID and a pass-word is revealed by executing the log-in with secret procedure by the insertion of an ID card.

CONSTITUTION: A main memory 6 of a terminal has a log-in procedure storing part 6a to store the log-in proceduce read from an ID card. The terminal, when a log-in request is inputted, reads the log-in procedure written beforehand and information such as a user ID and a pass-word from the ID card inserted by a card reading part 8. The pass-word (for example, group pass-word) different from the information from the ID card is inputted from a keyboard and the log-in is executed by the procedure read from

the ID card. When the writing request to the ID card occurs after the changing of the user ID or the pass-word, a card writing part 9 writes the new information or the procedure into the inserted ID card.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平4－267462

(43)公開日　平成４年(1992)９月24日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　15/00	３３０　Ｇ	7323－5L		
1/00	３７０　Ｅ	7927－5B		
Ｈ０４Ｌ　9/00				
9/10				
		7117－5K	Ｈ０４Ｌ　9／00	Ｚ

審査請求　未請求　請求項の数２（全　４　頁）　最終頁に続く

(21)出願番号　特願平3－28226

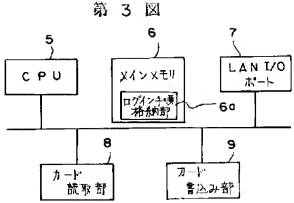
(22)出願日　平成３年(1991)２月22日

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号
(72)発明者　福留　直文
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内
(74)代理人　弁理士　大塚　康徳　(外１名)

(54)【発明の名称】　セキュリテイ方式

(57)【要約】
（目的）本発明は、ユーザＩＤやパスワード等の情報が知られてもセキュリテイを保護可能なセキュリテイ方式を提供することを目的とする。
（構成）ログインするための手順と情報とをＩＤカードから読み取る読取手段と、該手順と情報とに従ってログインするログイン手段とを備え、ＩＤカードの挿入により秘密の手順でログインが実行されることを特徴とする。更に、ログインするための手順を更新する手段と、該更新された手順をＩＤカードに書き込む手段とを備えることを特徴とする。

第３図



1

【特許請求の範囲】

【請求項1】　ログインするための手順と情報とをＩＤカードから読み取る読取手段と、該手順と情報とに従ってログインするログイン手段とを備え、ＩＤカードの挿入により秘密の手順でログインが実行されることを特徴とするセキュリティ方式。

【請求項2】　ログインするための手順を更新する手段と、該更新された手順をＩＤカードに書き込む手段とを更に備えることを特徴とする請求項1に記載のセキュリティ方式。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明はネットワークにおけるセキュリティ方式、特にＩＤカードを使用する場合のセキュリティ方式に関するものである。

【０００２】

【従来の技術】従来、ＩＤカードには個人を識別するための情報が入力されており、ビルの出入口でのチエツク等に用いられている。一方、ネットワークシステムにおいては、通常ホストコンピユータへのログインは端末からのキー入力で行うようになつている。

【０００３】

【発明が解決しようとしている課題】しかしながら、上記従来例では、ユーザＩＤやパスワード等の情報を部外者に知られやすいという欠点があつた。

【０００４】本発明は、前記従来の欠点を除去し、ユーザＩＤやパスワード等の情報が知られてもセキュリティを保護可能なセキュリテイ方式を提供する。

【０００５】

【課題を解決するための手段】この課題を解決するために、本発明のセキュリテイ方式は、ログインするための手順と情報とをＩＤカードから読み取る読取手段と、該手順と情報とに従つてログインするログイン手段とを備え、ＩＤカードの挿入により秘密の手順でログインが実行される。更に、ログインするための手順を更新する手段と、該更新された手順をＩＤカードに書き込む手段とを備える。

【０００６】かかる構成により、部外者にユーザＩＤやパスワード等の情報を容易には知られないようにしたものである。また、部外者が不正にＩＤカードを取得した場合でも、容易にはネットワークに侵入されないようにしたものである。

【０００７】

【実施例】図１は本発明のセキュリテイ方式を実施するネットワークシステムの構成を示すブロック図である。１はユーザに種々のサービスを提供するホストコンピユータ、２，３はサービスを受けるための端末、４はホストコンピユータ及び端末２，３を接続するＬＡＮである。

【０００８】図２はホストコンピユータ１のハードウエア構成を示すブロック図である。１１は本発明のセキュリテイ方式を含む種々のサービスをプログラムとして実行するＣＰＵ、１２は現在の各ユーザのパスワード及びグループパスワードを格納するパスワードテーブル、１３はプログラムをロードするためのメインメモリであると共に、ユーザのＩＤカードに書き込むための最新のログイン手順を記憶する最新ログイン手順記憶部１３ａを有する。１４はＬＡＮとの間のデータの入出力を制御するためのＬＡＮ I/Oポートである。

2

【０００９】図３は端末２，３のハードウエア構成を示すブロック図である。５は図５に示すようなソフトウエアをプログラムとして実行するＣＰＵ、６はプログラムをロードするためのメインメモリであると共に、ユーザのＩＤカードから読み込んだログイン手順を格納するログイン手順格納部６ａを有している。７はＬＡＮとの間のデータの入出力を制御するためのＬＡＮ I/Oポート、８はＩＤカードからログインの手順と情報とを読取るためのカード読取り部、９は新しい手順と情報とをＩＤカードに書込むためのカード書込み部、１０はパスワード等を入力するためのキーボードである。

【００１０】図４はホストコンピユータ１上で動作するソフトウエアのモジユール構成図である。図５は端末２，３上で動作するソフトウエアのモジユール構成図である。ここで、ＴＣＰ(Transmission Control Protocol)，ＩＰ(Internet Protocol)，ＬＬＣ(Logical Link Control)，ＤＬＣ(DataLink Control) であり、以下に簡単に説明する。

【００１１】ＴＣＰ／ＩＰは、アメリカ国防省がコンピュータネットワークを信頼性の高いものにするために作ったプロトコルである。ＴＣＰは、ネットワークに存在する２つのノード間をエンド・ツー・エンドで接続し、アプリケーション・プログラムに高品質で信頼性の高い通信機能を提供するための手順であり、順序制御，フロー制御などの機能を持つている。ＯＳＩでは第４層のトランスポート層および第５層のセツシヨン層に相当する。ＩＰは、複数のネットワーク間で途中のネットワークの際を吸収し、２つのノード間に透過な経路を作るための手順であり、グローバルなアドレスの割り付け，ルーテイング（経路選択）などの機能を持つている。ＯＳＩでは第３層のネットワーク層に相当する。

【００１２】ＬＬＣ／ＤＬＣは、ＩＥＥＥ８０２委員会で制定されたＬＡＮのデータリンク層のためのプロトコルである。ＬＬＣは、通信媒体の際を吸収し均一な隣接ノード間でのデータ転送機能を提供するための手順である。ＯＳＩでは第２層のデータリンク層の上位副層に相当する。ＤＬＣは、通信媒体ごとに異なるデータ転送機能を提供するための手順であり、例えばイーサネットの場合はＩＥＥＥ８０２．３のように、ＩＥＥＥでその手順の内容が規定されている。ＭＡＣ(Media Access Control)と呼ばれることもあり、ＯＳＩでは第２層の下位副

3

層に相当する。なお、ＯＳＩとの関係を示すと、次のようになる。ＯＳＩ　　ＬＡＮ

第７層　アプリケーション
第６層　プレゼンテーション
第５層　セッション　　ＴＣＰ
第４層　トランスポート　　ＴＣＰ
第３層　ネットワーク　　ＩＰ
第２層　データリンク　　ＬＬＣ／ＤＬＣ
第１層　フィジカル

図６，図７は端末上のソフトウエアの動作を示すフローチャートである。以下、このフローチャートに従って、本実施例の動作手順を説明する。

【００１３】まず、端末のシステム立上げ後は、ステップＳ１でユーザからの要求待ちの状態となっている。ここで、ユーザからログイン要求が入力されるとステップＳ３からＳ６に進んで、カード読取り部８で挿入されたＩＤカードから予め書込まれていたログイン手順とユーザＩＤやパスワード等の情報とを読取り、ステップＳ７ではＩＤカードからの情報とは別のパスワード（例えばグループパスワード）をキーボードから１０から入力させ、ステップＳ８で読みとられた手順でログインを実行する。

【００１４】ログイン手順が正常に終了、つまりログインできた場合には、ステップＳ９からＳ１に戻り、再び要求待ちの状態に戻る。また、手順の途中でパスワード入力ミス等正常に終了できなかった場合には、ステップＳ１０でエラー処理を行った後にステップＳ１に戻り、要求待ちの状態に戻る。

【００１５】また、ユーザＩＤあるいはパスワードの変更等を行った後に、ＩＤカードへの書込み要求が発生した場合は、ステップＳ２からＳ５に進んでカード書込み部９により挿入されているＩＤカードに新しい情報あるいは手順を書込んだ後にステップＳ１に戻り、要求待ちの状態に戻る。

【００１６】ログイン及びカード書込み以外の要求が発

4

生した場合には、ステップＳ４でその要求に対応した処理を行った後に、ステップＳ１に戻り要求待ちの状態に戻る。

【００１７】

【発明の効果】本発明により、ユーザＩＤやパスワード等の情報が知られてもセキュリテイを保護可能なセキュリテイ方式を提供できる。

【００１８】すなわち、ログインする手順と必要な情報をＩＤカードに入力する手段と、ＩＤカードからその手順と情報を読取って実行してホストにログインする手段を端末に設けたことにより、部外者にユーザＩＤやパスワード等の情報を知られにくくするとともに、ログイン時の操作を簡単にする効果がある。また、ログイン時に別にパスワードを入力する手段を端末に設けたことにより、部外者が不正にＩＤカードを取得した場合でも容易にはネットワークに侵入できないという効果がある。

【図面の簡単な説明】

【図１】本発明のセキュリテイ方式を実施するネットワークシステムの構成を示すブロック図である。

【図２】ホストコンピュータのハードウエア構成を示すブロック図である。

【図３】端末のハードウエア構成を示すブロック図である。

【図４】ホストコンピュータ上で動作するソフトウエアのモジュール構成図である。

【図５】端末上で動作するソフトウエアのモジュール構成図である。

【図６】，

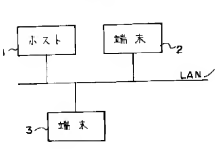
【図７】端末上のソフトウエアの動作手順を示すフローチャートである。

【符号の説明】

１…ホストコンピュータ、２，３…端末、４…ＬＡＮ、５…ＣＰＵ、６…メインメモリ、６ａ…ログイン手順格納部、７…ＬＡＮ Ｉ/Ｏポート、８…カード読取り部、９…カード書込み部、１０…キーボード、１１…ＣＰＵ、１２…パスワードテーブル、１３…メインメモリ、１３ａ…最新ログイン手順記憶部、１４…ＬＡＮ Ｉ/Ｏポート

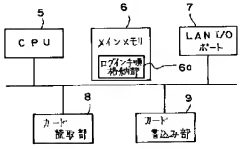
【図１】

第１図



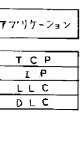
【図３】

第３図



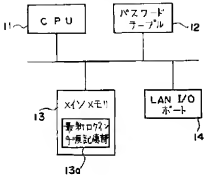
【図５】

第５図



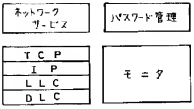
【図2】

第 2 図



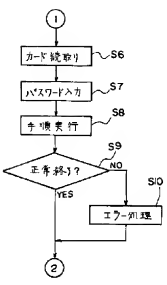
【図4】

第 4 図



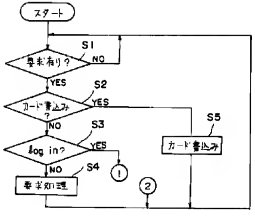
【図7】

第 7 図



【図6】

第 6 図



フロントページの続き

(51)Int.Cl.[5]	識別記号	庁内整理番号	FI	技術表示箇所
H04L 9/12				